

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----	x	
	:	
UNITED STATES OF AMERICA	:	
	:	
- v. -	:	S1 13 Cr. 834 (PKC)
	:	
ALEX YÜCEL,	:	
a/k/a "Alex Yucel,"	:	
a/k/a "Alex Yucle,"	:	
a/k/a "Alex Yuecel,"	:	
a/k/a "marjinz,"	:	
a/k/a "Victor Soltan,"	:	
	:	
Defendant.	:	
-----	x	

GOVERNMENT'S SENTENCING MEMORANDUM

PREET BHARARA
United States Attorney for the
Southern District of New York
One St. Andrew's Plaza
New York, New York 10007

DANIEL S. NOBLE
Assistant United States Attorney
- Of Counsel -



U.S. Department of Justice

*United States Attorney
Southern District of New York*

*The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007*

June 12, 2015

BY ECF & ELECTRONIC MAIL

The Honorable P. Kevin Castel
United States District Judge
Southern District of New York
Daniel Patrick Moynihan United States Courthouse
500 Pearl Street
New York, New York 10007

**Re: United States v. Alex Yücel,
S1 13 Cr. 834 (PKC)**

Dear Judge Castel:

The Government respectfully submits this letter in advance of sentencing of Alex Yücel (the “defendant”) scheduled for Friday, June 19, 2015 at 4:00 p.m., and in response to the defendant’s sentencing memorandum filed June 6, 2015 (“Def. Mem.”). The United States Probation Office (“Probation Office”) has calculated the applicable United States Sentencing Guidelines (“Guidelines” or “U.S.S.G.”) range to be 70 to 87 months’ imprisonment, as set forth in the Presentence Investigation Report dated May 11, 2015 (the “PSR”). The Government respectfully submits that a sentence within that Guidelines range is sufficient, but not greater than necessary, to achieve the purposes of sentencing in this case.

BACKGROUND

A. The Blackshades Remote Access Tool (“RAT”)

As set forth in detail in the PSR, between 2010 and 2013, an organization known as “Blackshades” sold malware to thousands of cybercriminals throughout the world. The leader of the Blackshades organization was the defendant, a Swedish national, who used the online pseudonym “Marjinz.” (PSR ¶ 33). The defendant was the owner and operator of the Blackshades business and the primary software engineer. (*Id.*) The defendant controlled and maintained the Blackshades server infrastructure, hired, fired, and paid employees, periodically updated the Blackshades suite of malware in response to customers’ comments and requests, and retained the bulk of the proceeds from the sale of Blackshades malware. (*Id.*).

Blackshades’ flagship product was the Remote Access Tool, or “RAT,” a sophisticated piece of malware that enabled cybercriminals remotely and surreptitiously to

Hon. P. Kevin Castel

June 12, 2015

Page 2

control other individuals' computers through the internet. (PSR ¶ 13).¹ The Blackshades organization sold the RAT for approximately \$40 per license. (PSR ¶ 16). The RAT was marketed in online forums, such as HackForums.net, as a product that conveniently combined the features of several different types of hacking tools. For instance, one online advertisement read:

Deciding between a RAT, a host booter, or controlling a botnet has never been easier.² With Blackshades . . . you get the best of all three – all in one with an easy to use, nice looking interface.

Even better, Blackshades . . . does a lot of work for you – it can automatically map your ports, seed your torrent for you, and spread through AIM, MSN, ICQ, and USB devices. (PSR ¶¶ 16-18).

Once a user had purchased a license for the Blackshades RAT, the infection of victims' computers could be accomplished in a few ways, including tricking victims into clicking on a link contained in an email or hiring others to install the RAT on the victim's computer, which at times Blackshades itself offered to do for an additional fee. (PSR ¶ 19). The RAT also contained tools known as "spreaders" that helped users of the RAT infect victim computers by using computers that had already been infected further to spread the RAT. (PSR ¶¶ 20-22). Unlike legitimate remote access tools used by IT administrators, the Blackshades RAT did not require victims' consent prior to installation of the RAT, or notify victims when a remote session was active on their computers.

¹ In addition to the RAT, the Blackshades organization had, from time to time, also sold software called "Blackshades Crypter," a program designed to make the RAT undetectable by anti-virus software; "Blackshades Stealth," a version of the RAT coded in certain programming languages that allowed the RAT to be controlled by computers using an Apple operating system in addition to PCs; and "Blackshades Fusion," malware designed to steal passwords, launch distributed denial of service ("DDoS") attacks, and capture webcam feeds, among other things. A DDoS attack occurs when a large group of remotely controlled computers (sometimes consisting of millions of computers) known as "bots" are instructed simultaneously to request information from a targeted computer. The targeted computer is so overwhelmed by such simultaneous requests that its ability to respond to legitimate requests is significantly slowed or temporarily stopped.

² A "host booter" is a tool that can be used to launch a denial of services ("DoS") attack, typically in the context of online video games. It disconnects or "boots" a person from a "host" (e.g., an online video game platform) and is typically done to cheat at the video game. A "botnet" typically refers to a network of infected computers or "bots."

Hon. P. Kevin Castel

June 12, 2015

Page 3

Upon infection of a victim's computer, the RAT user had free rein to, among other things: access, view, and steal the victim's documents, photographs, and other files; "hijack" the victim's files by requiring a ransom to "unlock" the files; employ the infected computer as a "bot" in a distributed denial of service ("DDoS") attack; record a victim's keystrokes through a "keylogger" to steal the victims' passwords and credit card numbers; and activate the victim's web camera to take still photographs or obtain a live feed of the victim without his or her knowledge. (PSR ¶¶ 25-29). All of these features could be controlled through the RAT's graphical interface, which allowed users easily to view and navigate all of the victim computers that they had infected. (PSR ¶¶ 23-24). Attached as Exhibit A are screenshots of the RAT user interface and certain RAT features, including the file hijacker, DDoS controller, and webcam controller.

In the course of its investigation of Blackshades, the Federal Bureau of Investigation ("FBI") seized and searched the Blackshades server, pursuant to a search warrant. (PSR ¶ 37). A review of the records stored on the server revealed that there were more than 6,000 Blackshades customer accounts located in more than 100 countries. (PSR ¶ 38). Based on records obtained from various electronic payment processors, the Blackshades organization generated at least \$350,000 in revenues from sales of the RAT between September 2010 and April 2014. (PSR ¶ 35).

B. Procedural History and Guidelines Calculation

On or about November 25, 2013, a grand jury in this District returned a five-count Superseding Indictment S1 13 Cr. 834 (PKC) (the "Superseding Indictment") against the defendant. Count One charged the defendant with conspiracy to commit computer hacking, in violation of 18 U.S.C. § 1030(b). Count Two charged the defendant with substantive computer hacking, and aiding and abetting the same, in violation of 18 U.S.C. §§ 1030(a)(5)(A), 1030(c)(4)(B)(i) and (c)(4)(A)(i)(VI), and 2. Count Three charged the defendant with access device fraud conspiracy, in violation of 18 U.S.C. § 1029(b)(2). Count Four charged the defendant with substantive access device fraud, and aiding and abetting the same, in violation of 18 U.S.C. §§ 1029(a)(4) and 2. Count Five charged the defendant with aggravated identity theft, and aiding and abetting the same, in violation of 18 U.S.C. §§ 1028A and 2.

On November 27, 2013, pursuant to the United States' provisional arrest request, the defendant was arrested in Moldova. On May 28, 2014, the defendant was extradited from Moldova to the United States. (PSR ¶ 53). In the order authorizing extradition, however, Moldova limited the defendant's extradition to Counts Two and Four of the Superseding Indictment – the substantive computer hacking and access device fraud charges.

On February 18, 2015, the defendant appeared before Your Honor and pleaded guilty, pursuant to a plea agreement, to Count Two of the Superseding Indictment. (PSR ¶ 8). In

Hon. P. Kevin Castel

June 12, 2015

Page 4

the plea agreement, the parties stipulated that the applicable Guidelines range is 70 to 87 months' imprisonment. (PSR ¶ 9(j)).

The Probation Office has calculated the advisory Guidelines range to be 70 to 87 months' imprisonment, which is the same as the parties' stipulated Guidelines range in the plea agreement. (PSR ¶¶ 9, 98). The Probation Office recommends a sentence at the low-end of the Guidelines range of 70 months' imprisonment. (PSR at 21 (Sentencing Recommendation)).

C. Related Cases

In the course of its investigation, the FBI arrested two other individuals who worked with the defendant in operating the Blackshades business. First, the FBI arrested the co-creator and an administrator of the Blackshades RAT, "Xviseral," who pleaded guilty to felony computer hacking charges and is pending sentencing before this Court in July 2015. Second, the FBI arrested Brendan Johnston, who worked for the defendant as an administrator between the summer of 2011 and September 2012. Johnston's primarily responsibilities were to market and sell the RAT and oversee customer service representatives to provide troubleshooting and technical support for RAT users. Johnston has pleaded guilty to conspiracy to commit computer hacking and is scheduled to be sentenced by the Honorable Jesse M. Furman on June 18, 2015.

In addition, the FBI arrested three Blackshades customers in the New York/New Jersey area – Juan Sanchez, Kyle Fedorek, and Marlen Rappa – all of whom have pleaded guilty and been sentenced. Sanchez used the RAT primarily to spy on his girlfriend; Sanchez pleaded guilty to a misdemeanor computer hacking offense and was sentenced on December 23, 2014 by the Honorable James C. Francis IV to one year of probation. Fedorek used the RAT primarily to steal victims' usernames and passwords for various financial, email, and social networking accounts; Fedorek pleaded guilty to a felony computer hacking offense and was sentenced on February 19, 2015 by the Honorable Vernon Broderick to a term imprisonment of two years. Rappa used the RAT primarily to steal photographs from victims' – mostly young women's – computers and spy on them using the RAT's webcam capture feature; Rappa pleaded guilty to a felony computer hacking offense and was sentenced on April 22, 2015 by the Honorable Valerie E. Caproni to a term of imprisonment of 12 months and one day.

D. Victim Notification and Remediation

The Government took various steps during its investigation and takedown of the Blackshades organization to attempt to identify and provide remediation to victims, including those individuals whose computers the defendant helped others to infect with the RAT.

Hon. P. Kevin Castel

June 12, 2015

Page 5

Unfortunately, for the reasons explained below, the FBI was unable to identify particular victims of the Blackshades organization.

During the investigation, the Government obtained court orders to install pen registers and trap-and-trace devices (“pen/trap devices”) on certain Blackshades customers’ Internet connections in order to identify the Internet protocol (“IP”) addresses of computers that were communicating with the Blackshades customers’ computers. By applying various filters to those IP addresses, the Government identified the IP addresses that were most likely to belong to victims. The Government then issued Grand Jury subpoenas to obtain subscriber information for those IP addresses in order to determine their physical locations. After identifying locations in the New York City area, FBI agents visited approximately ten different potential victims and attempted to obtain consent to search those computers for evidence of Blackshades infection. Unfortunately, none of the potential victims were willing to allow federal agents examine their computers. Thus, this house-to-house approach was not practicable.

In preparation for the takedown, which involved coordinated law enforcement actions in over a dozen countries, the Government applied for search warrants to seize electronic evidence from certain Blackshades customers’ residences. A search of these computers revealed that victims’ Blackshades-infected computers were identified on the RAT users’ computer only by the name that the victim gave to his or her computer, such as “Jane’s computer.” Not surprisingly, none of the computer names contained the victims’ full true name or other identifiers. The RAT also did not capture (or at least did not store) the IP addresses of the victims’ computers, information that might otherwise have indicated at least the physical locations of the victims, such as whether they were in the United States or abroad.

At the time of the takedown, the Blackshades organization had approximately 2,000 active customer accounts, each of which used a unique domain name to communicate with victims’ computers (collectively, the “Customers’ Domains”). In preparation for the takedown, and in a further effort to identify Blackshades victims, the Government applied for a court order to redirect all communications to the Customers’ Domains to an FBI-controlled computer (the “FBI Computer”). The Government also applied for an Order authorizing the FBI to install a pen/trap device on the FBI Computer in order to capture the source IP addresses of computers that attempted to communicate with the Customers’ Domains. However, an extremely large volume of IP addresses contacted the FBI Computer within the first hour, most of which were unlikely to have been IP addresses of victim computers. For example, IP addresses that contacted the FBI Computer included many that appeared to belong to so-called web crawlers, or computers that systematically browse the Internet, typically in order to index websites. Thus, identifying true victims from the huge number of IP addresses contacting the FBI Computer was also not practicable.

Notably, although the redirection of Customers’ Domains and IP Addresses was unsuccessful in identifying victims, it did permanently disrupt the connection between victims’

Hon. P. Kevin Castel
 June 12, 2015
 Page 6

computers and Blackshades Customers' Domains. This effort, coupled with the seizure of the Blackshades organization's server infrastructure, made it impossible for Blackshades customers, such as the defendant, to continue to access victims' computers.

Finally, the Government also took steps to educate the public about Blackshades and possible remedial action. For example, information about the Blackshades investigation and how to determine if a computer might be infected by Blackshades was posted on the FBI's website.³ The Government also encouraged private industry to develop a Blackshades removal tool and publicize the existence of Blackshades on their websites.⁴

APPLICABLE LAW

The United States Sentencing Guidelines still provide strong guidance to the Court following United States v. Booker, 543 U.S. 220 (2005), and United States v. Crosby, 397 F.3d 103 (2d Cir. 2005). Although Booker held that the Guidelines are no longer mandatory, it also held that the Guidelines remain in place and that district courts must "consult" the Guidelines and "take them into account" when sentencing. Booker, 543 U.S. at 264. As the Supreme Court stated, "a district court should begin all sentencing proceedings by correctly calculating the applicable Guidelines range" — that "should be the starting point and the initial benchmark." Gall v. United States, 552 U.S. 38, 49 (2007).

After that calculation, however, a sentencing judge must consider seven factors outlined in 18 U.S.C. § 3553(a): "the nature and circumstances of the offense and the history and characteristics of the defendant," 18 U.S.C. § 3553(a)(1); the four legitimate purposes of sentencing, see id. § 3553(a)(2); "the kinds of sentences available," id. § 3553(a)(3); the Guidelines range itself, see id. § 3553(a)(4); any relevant policy statement by the Sentencing Commission, see id. § 3553(a)(5); "the need to avoid unwarranted sentence disparities among defendants," id. § 3553(a)(6); and "the need to provide restitution to any victims," id. § 3553(a)(7). See Gall, 552 U.S. at 50 & n.6.

In determining the appropriate sentence, Section 3553(a) directs judges to "impose a sentence sufficient, but not greater than necessary, to comply with the purposes" of sentencing, which are:

(A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense;

³ See, e.g., <http://www.fbi.gov/news/stories/2014/may/international-blackshades-malware-takedown>; <http://www.fbi.gov/news/stories/2014/may/international-blackshades-malware-takedown/could-your-computer-be-infected-by-blackshades>.

⁴ See, e.g., <http://www.symantec.com/connect/blogs/blackshades-coordinated-takedown-leads-multiple-arrests>.

Hon. P. Kevin Castel

June 12, 2015

Page 7

(B) to afford adequate deterrence to criminal conduct;

(C) to protect the public from further crimes of the defendant; and

(D) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner.

18 U.S.C. § 3553(a)(2).

DISCUSSION

Application of the Section 3553(a) factors to the facts of this case supports a sentence within the advisory Guidelines range. Because of the serious nature of the defendant's conduct; the long period of time during which he designed, administered, and sold Blackshades malicious software; his leadership role; the need to deter the defendant and others from distributing and using harmful malware like the Blackshades RAT; and the absence of any compelling mitigating circumstances, the Government submits that a sentence within the advisory Guidelines range of 70 to 87 months' imprisonment is warranted.

First, a sentence within the applicable Guidelines range is necessary to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment. See 18 U.S.C. § 3553(a)(2)(A). It cannot seriously be disputed that the defendant's criminal conduct was serious. For over three years, the defendant designed, developed, marketed, and sold the Blackshades RAT and other malicious software to thousands of users in more than 100 countries. The defendant was the primary engineer of the Blackshades malware, the leader of the Blackshades business, and the person who primarily profited from the sale of the malware. In his role as the leader of the Blackshades business, the defendant hired and paid other administrators, like Brendan Johnston, who, in turn, oversaw a team of customer support personnel to provide technical assistance to RAT users. Through his actions, the defendant directly enabled thousands of RAT users to infect and take control of victims' computers without the victims' knowledge or consent.

The substantial harm caused by the defendant's conduct is illustrated by the cases of two Blackshades customers who were prosecuted in this District: Kyle Fedorek and Marlen Rappa. Fedorek used the Blackshades RAT, which he purchased from the defendant and his associates, to infect over 400 victims' computers. Fedorek used the Blackshades RAT to obtain approximately 90 unauthorized access devices in the form of financial account credentials, like usernames and passwords. Rappa used the Blackshades RAT to infect almost 100 victims' computers, from which he downloaded thousands of personal photographs, videos, and other files. Rappa also used the Blackshades webcam feature to spy on his victims and take still screenshots of them, including when they were naked and having sex. Fedorek's and Rappa's

Hon. P. Kevin Castel

June 12, 2015

Page 8

egregious invasions of their victims' privacy and theft of their victims' financial and personal information illustrates the types of harms that flowed directly from the defendant's design, development, and distribution of the Blackshades RAT.

In his sentencing memorandum, the defendant makes the outrageous claims that Blackshades was a legitimate IT tool that could be used by computer network administrators "to perform perfectly legal activities" and that there were only isolated "instances of misuse and abuse" of the Blackshades RAT. (Def. Mem. 2-3). Although he insists that he is not "stepping away" from his guilty plea (Def. Mem. 2-3), the defendant's persistent denial of the illicit nature of the Blackshades RAT not only strains credulity, but puts the defendant dangerously close to the line of failing to demonstrate full acceptance of responsibility for his conduct. Despite the defendant's contentions, the illicit nature of the Blackshades RAT is immediately apparent from its own features, including the "DDoS" controller, "file hijacker," and "spreader" tools. Indeed, standard anti-virus programs frequently included Blackshades in their lists of malware to block. In addition, unlike legitimate remote access tools, victims were not asked for their consent before the RAT was installed on their computers, nor were victims notified when the RAT was running on their computers. For instance, victims clearly were not notified when Marlen Rappa activated their webcams using the Blackshades RAT and took photographs of them engaged in sexual acts. It is also telling that the Blackshades RAT was advertised on HackForums.net, a site regularly frequented by computer hackers, including the defendant, and was specifically marketed as an "all-in-one" computer hacking tool comprising a remote access controller, booter, and DDoS controller.

In addition to the seriousness of the offense, a Guidelines sentence is also necessary to achieve adequate deterrence in this case. See 18 U.S.C. § 3553(a)(2)(B). As a general matter, computer hacking is becoming an ever more prevalent and pernicious threat in our society. Using inexpensive and easy-to-use hacking tools such as the Blackshades RAT (which only cost \$40 to purchase on the internet), even low-skilled cyber criminals can obtain access to and control over others' computers. With such unfettered access, cyber criminals can steal the victims' personal and financial information, spy on them, or enlist the victims' computers to commit additional cybercrimes, such as DDoS attacks. In addition, given the anonymity of the Internet and the proliferation of tools available to cyber criminals to evade law enforcement, it is often difficult to identify, much less apprehend, cyber criminals. Thus, significant penalties are necessary to send a message that the illegal distribution and use of malware will not go unpunished when cyber criminals are caught.

In addition, a substantial sentence is warranted in order to achieve specific deterrence as to this defendant. The PSR states that the defendant was raised in a two-parent, middle-class family in Stockholm, Sweden. (PSR ¶¶ 80-81). The defendant was educated, played hockey growing up, has enjoyed good health, and worked as a computer programmer for his father's company. (PSR ¶¶ 81, 88, 91-92). Yet, despite the fortunate circumstances of his upbringing, the defendant turned to selling malicious software in order to make money. The

Hon. P. Kevin Castel

June 12, 2015

Page 9

defendant's greed and desire to profit from crime is revealed in the following email exchange from October 17, 2010 with Xvisceral, which was included in the Government's Extradition Request to Moldova: "Yo. look dude. we can become rich :P" The defendant then provided a link to a website and told Xvisceral to "check that. people selling dumps [*i.e.*, lists of credit card numbers and other personal identification information]. i got thousands of these. and people sell them like 15-40 usd/ each. i can sell them for 10 each. and 5 if they buy over 100." The defendant also explained how he obtained the credit card data: "I have backdoored a maxican [sic] professional skimmer . . . and he is skimming atms [automated teller machines]." ⁵ The defendant then provided Xvisceral a particular credit card number as proof that he possessed the credit cards. He further wrote that, using "a machine called MSR206 and an empty credit card," the account information could be copied "to the empty card" and then the criminal could "go to any shop and use it." (Extradition Request ¶ 27). ⁶ The fact that the defendant was willing to engage in such blatant criminal activity simply for profit, despite all the advantages of his middle-class upbringing, educational, and employment opportunities, demands a significant term of imprisonment to deter the defendant from ever again turning to computer hacking or other criminal activity to enrich himself.

In requesting a significant downward variance, the defendant places much emphasis on the circumstances of the "punishment" to which he has been subjected already. (See Def. Mem. 5-6, 15-16). Although "courts have granted relief generally where the conditions in question are extreme to an exceptional degree and their severity falls upon the defendant in some highly unique or disproportionate manner," United States v. Mateo, 299 F. Supp. 2d 201, 211 (S.D.N.Y. 2004) (citing cases), the defendant cites no such extreme or unique conditions in this case. The defendant contends that his detention has been "more onerous" than usual because of (i) the "traumatic" circumstances of his extradition from Moldova (Def. Mem. 5-6, 15); (ii) the "harsh" conditions of his confinement at the MCC, such as the "lack of programming" and "lack of exposure to sunlight and the outside" (*id.* at 3, 15-16); (iii) his claimed, but undocumented, "bouts of depression and anxiety" (*id.* at 5); and (iv) the loss of family and community support (*id.* at 15). But the circumstances that the defendant cites in his submission can hardly be characterized as "extreme to an exceptional degree," and there is certainly no suggestion in the record that they affect the defendant uniquely or disproportionately. Indeed, such conditions befall most, if not all, defendants who are extradited from foreign countries to this District to face charges of serious violations of United States law. Although the circumstances of the defendant's pre-trial detention are a factor the Court may consider, this factor simply cannot bear the weight that the defendant urges.

⁵ As explained in the Extradition Request, "backdooring" is often a general term for successfully compromising another person's computer, and "skimming" refers to surreptitiously capturing credit card numbers, often by installing an unauthorized magnetic stripe reader on an otherwise legitimate location.

⁶ In the context of these chats, an "MSR" likely referred to a magnetic stripe reader, which is used to extract data stored on the magnetic stripes of credit cards.

Hon. P. Kevin Castel
 June 12, 2015
 Page 10

The defendant also argues for a downward variance based on Proposed Amendments to the victim enhancement provision of Section 2B1.1 of the Sentencing Guidelines, which, absent Congressional action to the contrary, will go into effect on November 1, 2015.⁷ Under the Proposed Amendments, there would only be a two-level increase, as opposed to the six-level increase under the present Guidelines, because the Government could not prove by a preponderance of evidence that a sufficient number of victims suffered “substantial financial hardship”⁸ so as to warrant an enhancement above two levels. *Compare* Proposed Amendment to U.S.S.G. § 2B1.1(b)(2)(A) (enhancements over two levels based not on total number of victims alone, but on number of victims who suffered “substantial financial hardship”), *with* U.S.S.G. § 2B1.1(b)(2)(A) (2014) (enhancement based only on number of victims). The defendant’s argument is unavailing.

Section 3553(a) provides that the sentencing court “shall consider,” among other things, the “sentencing range” established by the Guidelines that are “in effect on the date the defendant is sentenced.” 18 U.S.C. § 3553(a)(4)(A)(ii) (emphasis added); *see Dorsey v. United States*, 132 S. Ct. 2321, 2332 (2012); *see also United States v. Brooks*, 732 F.3d 148, 149 (2d Cir. 2013) (“Generally, sentencing courts are required to apply the Guidelines Manual in effect on the date that the defendant is sentenced.”). Thus, although the Court may consider the Proposed Amendments to Section 2B1.1, they do not affect the Guidelines range calculated by the Probation Office and agreed to by the parties that the Court must consider in imposing sentence under Section 3553(a). Moreover, the sheer number of individuals who were victimized as result of the defendant’s distribution of the Blackshades RAT and the types of non-monetary harms that they suffered due to the egregious violations of their privacy (which are not fully accounted for by the current or soon-to-be amended victim enhancement under Section 2B1.1), weigh heavily against the downward variance that the defendant requests based on the Proposed Amendments.

⁷ The official text of the amendments are available at http://www.ussc.gov/sites/default/files/pdf/amendment-process/official-text-amendments/20150430_Amendments.pdf. A “reader friendly” version of the amendments, which contains redlined changes comparing the presently applicable amendments to the Proposed Amendments, is available at http://www.ussc.gov/sites/default/files/pdf/amendment-process/reader-friendly-amendments/20150430_RF_Amendments.pdf.

⁸ The Proposed Amendments add a non-exhaustive list of factors to be considered in determining whether the offense caused “substantial financial hardship,” including: becoming insolvent; filing for bankruptcy; suffering substantial loss of a retirement, education, or other savings or investment fund; making substantial changes to employment; making substantial changes to living arrangements; or suffering substantial harm to the victim’s ability to obtain credit.


Hon. P. Kevin Castel
June 12, 2015
Page 11

CONCLUSION

For the foregoing reasons, the Government respectfully requests that the Court impose a sentence within the advisory Guidelines range of 70 to 87 months' imprisonment. In addition, at sentencing the Government will submit a proposed Forfeiture Order for the Court's consideration.

Respectfully submitted,

PREET BHARARA
United States Attorney

By: 
Daniel S. Noble
Assistant United States Attorney
(212) 637-2239

Encl.

cc: Brad Henry, Esq. (by ECF & electronic mail)